European Research Studies
Volume XX, Issue 1, 2017

pp. 36 - 48

Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them

Natalia G. Vovchenko[1], Evgeniy N. Tishchenko[2], Tatiana V. Epifanova[3], Mark B. Gontmacher[4]

Abstract:

The article reveals the essential characteristic of virtual currencies. The estimate is given to the development of risks and threats to national security, combating laundering of criminal money and terrorism financing, which are formed under the conditions of the growing interest in virtual currencies, including Bitcoin.

It is suggested to minimize negative effect arising in this relation. Methods are proposed to adapt the management center in the virtual currency infrastructure.

Key Words: *Bitcoin, national security, money laundering, crypto-currency, virtual currency, Bitcoin, data-management center, peer network.*

[1]*Natalia G. Vovchenko, Prof., Dr Sci (Econ), Department of Finance, Rostov State Economic University (RINH), Rostov-on-Don.*
[2]*Evgeniy N. Tishchenko Prof., Dr Sci (Econ), Department of Informational technologies and information protection , Rostov State Economic University (RINH), Rostov-on-Don*
[3]*Tatiana V. Epifanova, Dr Sci (Econ), Department of Civil Law, Rostov State Economic University (RINH), Rostov-on-Don.*
[4]*Mark B. Gontmacher, graduate student, Department of Finance, Rostov State Economic University (RINH), Rostov-on-Don.*

Introduction

Due to the rapid developments in spheres of financial innovation and information technologies, world space is being transformed into a global business system (Akopova and Przhedetskaya, 2016; Boldeanu and Tache, 2015; Dmitrishina and Uskov, 2015; Epifanova *et al.*, 2015; Fatai, 2015; Rusanov *et al.*, 2015; Rupeika-Apoga and Nedovis 2015; Thalassinos *et al.*, 2013; Thalassinos and Stamatopoulos, 2015; Thalassinos, 2007). The volume of electronic payments in recent years has grown significantly with the introduction of computers and information technology into virtually all spheres of daily activity. The volume of e-commerce in Russia in 2013 reached $ 13 bln, an increase of 35% as compared to 2012. At the end of 2013 about 7.2 million people in Russia have used e-wallets for payments and mutual settlements. The market volume of electronic purses is estimated at $9 billion in 2015, with an outlook to its exponential growth.

Dynamic changes in the world processes, particularly in the virtual economy sphere pose challenges to the national security system.

Rationale

According to the Decree of the President of the Russian Federation as of 31.12.2015, № 683 "On the Russian Federation National Security Strategy" national security – is a state of security for the individual, society and state from internal and external threats, which provides a realization of the constitutional rights and freedoms, decent quality of life, sovereignty, independence, statehood and territorial integrity, as well as sustainable economic and social development of the Russian Federation. National security also includes information security.

The National Security Strategy it is stated that amongst the main strategic risks for the economic sphere of Russian Federation in long term are: high dependence on the external economic environment, the lag in the development and implementation of advanced technologies, the vulnerability of the national financial system from actions of non-residents, as well as speculative foreign capital.

In this regard, the system is required to provide protection mechanisms, including the regulatory, legal and organizational support of the development of economic processes that meet modern international realities and minimize the risks of illegal activities. Main issue is the balance between the state measures, which can potentially harm the virtual economy, and legislation enabling participants to carry out operations with virtual currency for criminal purposes.

The economic system is dynamic, committed to the development and includes the use of new technological opportunities. This aspect has led to the need for continuous improvements in the national security measures.

In particular, the emergence of virtual currencies (cryptocurrency) is actively discussed globally, the most famous of these is the Bitcoin. The Bitcoin is widely spread in many countries, competing with the national currencies, such the euro and the dollar. This Bitcoin is not secured by any assets, and is not tied to any world currency - its rate is determined by supply and demand, making Bitcoin exchange rate volatile, yet objective at the same time. All Bitcoin transactions records are kept in the public domain, but without information disclosure of the actual participants, turning this innovative payment instrument into one of the mediums facilitating criminal activity. Currently, every 10 minutes 25 new Bitcoins are added to the network.

In other words, if the user runs a special program his/her computer solves a mathematical problem. Correct solution will earn some amount of Bitcoin to the user. The exchange rate of Bitcoin is unstable, last year it ranged from $100 to $1100, with recent months level about $600. According to official statistics, the total volume of issued Bitcoin is estimated at $8 billion.

Legal status of cryptocurrency, despite the widespread dissemination and use of the Internet, is not legally secured and requires detailed consideration not only by lawyers and economists, but first and foremost by software engineers.

The distinguishing characteristics of cryptocurrencies, including Bitcoins are: 1) the real purchasing power; 2) lack of security; 3) the official exchange rate in relation to the major world currencies; 4) decentralization -no single governing body of emission management and control; 5) the anonymity of the operations; 6) the absence of inflation, due to algorithmic limitations Bitcoin; 7) Bitcoin value is determined by supply and demand.

It is necessary to distinguish between electronic money and cryptocurrency in terms of their basic characteristics. Electronic money - is the storage and transmission of traditional currency and, most importantly, in economic terms, they retain their value for the transmission and storage of money that is available in an amount not less than that emitted by monetary value. Electronic money is a mechanism for an electronic transfer of fiat currency, i.e., they are used for electronic transfer of currency, have the status of legal medium of exchange. In this context, great importance is the fact that unauthorized transfers of cryptocurrency are outside the legal framework, which allows for the implementation of the unlawful acts.

The facts stated above form a threat to the national security. As stated in this strategy - a set of conditions and factors that create the possibility of direct or indirect damage to objectively significant needs of individuals, society and the state to ensure their protection and sustainable development.

A similar position is set out by the European Union, via an issued a warning regarding the risks associated with transactions in the virtual currency, pointing to the lack of legal regulation protecting consumers from the state and creates a risk of losing money.
According to the Report of the Group for Development of Financial Measures to Combat Money Laundering (hereinafter - FMCML), the turnover of the virtual currency has options of legitimate use as well as features that contain potential risks to the financial system. It is noted that legitimate cryptocurrency operations have the potential to improve the efficiency of payments and reduce the costs of payments and transfers of funds.

It is indicated that Bitcoin can function as a global currency, in which there are no exchange fees, which contributes to the development of the existing online payment systems. There are also investment strategies where cryptocurrencies such as Bitcoin can be utilized.

It is necessary to point out one more concept of Bitcoin that exhibits the greatest risk to national security. In particular, it is characterized by full anonymity Bitcoin system participants. This fact forms a stable foundation for the development of the illegal operations, including those related to the financing of terrorism and extremism.

Potential vulnerability to illegal operations by the virtual currency use is often pointed out by the world's financial experts in the field of combating money laundering. This is due to the fact that the virtual currency provides a higher degree of anonymity when compared to traditional methods of cashless payments. Infrastructure of virtual currency allows anonymous funding in the absence of direct interaction with clients as well as conducting operations through virtual exchange points, where the identification of the source of funding is not carried out properly.
Serious complications to the situation are the absence of the means and possibilities of establishing software, aimed at identifying and tracking ventures, bearing suspicious character. A further complication is widespread geographical distribution of services involving virtual currency. Thus, virtual currency is functioning in the system of complex infrastructure operations in which subjects are located in different jurisdictions.

Under such circumstances, the establishment of specific responsibilities for compliance with the system of counteraction to money laundering, as well as the implementation of supervisory and enforcement powers is very difficult.

An important note is that in modern conditions there are a number of states secretly supporting terrorist acts, including ISIS prohibited on the territory of the Russian Federation. Given the lack of adequate controls over transactions with Bitcoin, the risk of the anonymous transactions between entities financing terrorism is extremely high.

Current Research

In this regard, a number of researchers studying Bitcoin, as well as representatives of the business community have expressed the view on the need to develop control measures for the given socio-economic phenomenon.

Certainly banning virtual currency does not lead to the eradication of the problem. The need for technological development alternatives of financial instruments, which develop into virtual currencies, requires a system of measures, such as a fuzzy legal regulation, promoting legal violations in this area and growing shadow economy.

Amongst the weak points of new payment methods and the risks of their misuse for the purpose of money laundering and terrorist financing we can point out:
- High speed of cross-border movement of money in large volumes;
- Anonymous payments and "contactless" transactions carried out;
- Lack of adequate legal regulations of Internet payments.

To resolve the problems mentioned above, preserve the national security, as well as participate in the initiatives of the world's technology and global business, the proposals are:
1. To create an official national cryptocurrency issued by the central bank;
2. To create a system to license enterprises working with national cryptocurrency;
3. To identify customer reliability, taking into account the threshold amounts of transactions.
4. To create a centralized depository of cryptocurrency for security of Internet users (data center);
5. To create a system of ATMs for cryptocurrency exchange, thereby ensuring transparency and identification of users;
6. To create a program to improve the financial literacy, as well as include a section on the use of cryptocurrency.
7. To modernize the institutional business environment, taking into account trends in the developments of the virtual economy (regulatory, legitimate, cognitive aspect).

In one of the proposals mentioned above, and in addition to this list, it seems necessary to consider infrastructural characteristics and problems of functioning of virtual currencies in more detail.

All the currently known technology functioning virtual money has a topology of peer to peer networks, which has a high level of security and reliability. The key feature of this is the process of hashing of chain transaction units (blockchain). Therefore, in terms of control of operations, it is necessary to introduce the transaction management technology centers on the basis of data processing centers (DPC), which turn can also be organized in the form of peer to peer networks.

This raises another set of organizational problems related to resources of the data center as part of the infrastructure of virtual currency, which can be solved, using methods of adaptation.

Adaptation of processor nodes

Analyzing the situation of requests to the data center, we can assume that hosts of peer network produce a stream of transactions or tasks, time for the task completion is random, and the processor data center nodes for incoming requests, serve as service nodes. At the same time, you can determine the number of required data center nodes, using queuing theory.

The system described is a multichannel queuing system with rejections. Hosts of the network generate a random number of requests, software and hardware that is realized through data centers. Those have a number of sub-systems which service the application, in a random time interval.

Streams - a simple Poisson distribution

If the process that takes place in the service system involves marking, the system may have the following states: $S_0, S_1, ..., S_n$, where S_k - is the state where k -number of processes is launched (k-number of channels is busy).

Requests flow switches the system from current state, to a right state with the intensity **λ**. The probability of transition of the system into the right state (ignoring the adjacent), is rejected due to the fact that software and hardware implemented data center considers the number of requests. All simultaneous attempts to run the application are transferred to the queue status. The intensity of a certain flow of services that translates the system into the initial condition, changes regularly according to that state. If the system implements **k** number of service requests, then system can go to the state S_{k-1} - the case where any of the **k** network nodes completes the process. The total intensity of the flow will be $k\mu$.

The main problem that can be solved using the queuing system is determining the number of such service processor nodes (data center elements) that the maximum number of hosts had the opportunity to activate its own process.

The initial stage of solution is finding the intensity of the flow of requests **λ**. To do this, it is necessary to make sure that the frequency of requests corresponds to the simplest Poisson flow. It is necessary to calculate the observed frequencies, as well as to determine the theoretical frequencies. It is necessary to calculate the average rate given the fact that this process follows Poisson:

$$n_{cp} = \frac{\sum_{i=0}^{m} if_i}{\sum_{i=0}^{m} f_i},$$

where m - total number of values that an observed variable can take

f_i - frequency of the observed variable i

The theoretical frequencies are determined by:

$$f_n = (\sum_{i=0}^{m} f_i) \times \frac{(n_{cp})^n \times e^{-n_{cp}}}{n!},$$

Where m - total number of values that an observed variable can take

n_{cp} - average frequency;

f_i - frequency of the observed variable i

n - the value of frequency of the observed variable

Then, the system is switching the flow rate from the "right" state into the "left" state. In the system described, this variable may be defined as the average number of terminating processes per hour (average execution time).

While calculating this time it is necessary to conduct statistical surveys. During the observations, the time is determined throughout the working day, after which the selected hours are loaded and the average is calculated.

The next step is to determine the law of distribution of the observed values. At the same time we assume that we have a system of mass service with rejections (input stream is subject to Poisson distribution).

Taking into account the properties of the system, its performance indicators can be calculated using the Erlangs' formula for the probabilities (in limit):

$$p_0 = (1 + \rho + \frac{\rho^2}{2!} + ... + \frac{\rho^n}{n!})^{-1},$$

Given that:

$$\rho = \frac{\lambda}{\mu},$$

where p_0 - probability of each service channel being free (not busy)

p_n - probability of n channels being busy

μ - intensity of service flow of incoming requests

ρ - given intensity of the analyzed request flow determines mean number of requests that enter the system in the time interval that it takes to complete one request

λ - flow intensity of incoming requests

Given this, the probability of the mass service system rejecting is the marginal probabilities of all n channels of the system are busy:

$$P_{отк} = p_n = \frac{\rho^n}{n!} \times p_0 .$$

Therefore there can be found a relative capacity, so the probability of servicing the request:

$$Q = 1 - P_{отк_n} = 1 - \frac{\rho^n}{n!} \times p_0 .$$

Furthermore, absolute capacity (mean number of requests per unit of time) can be found using:

$$A = \lambda \times Q = \lambda(1 - \frac{\rho^n}{n!} p_0) .$$

Mean number of busy channels is calculated using:

$$\bar{k} = \frac{A}{\mu} = \rho(1 - \frac{\rho^n}{n!} \times p_0) .$$

Hence, in order to determine the required number of processor data center nodes it is necessary to determine such number of servers n, under which the value of the relative capacity is equal to the specified level of significance.

The value of the service flow rate of incoming orders in the system is determined by the formula:

$$\mu = 1/\overline{T}_{об} .$$

The described method of calculating the number of processing nodes allows us to determine the required quantity of such nodes as well as significantly reduce the cost of infrastructure for virtual currency.

Adapting temporary data center operation characteristics. Hardware and software components of the data center as the test objects have certain characteristics:

- The absence of a predetermined benchmark, to rank the test results against;
- A large complexity of hardware and software components and, therefore, the failure to develop a comprehensive testing algorithm;
- The complexity of the formalization of quality indicators of the testing process and the quality of the test object;
- The presence of logical and computational components that are characterized by dynamic structure.

The sources that discuss this particular issue contain mathematical models for building the data center, which can be taken as abstract benchmarks. However, in specific circumstances, many indicators are ambiguous for systems that implement different functions.

Algorithm of data center functions can be viewed as a sequence of elementary operations with the definition of timing parameters for their implementation. In simulations using standard software tools, it can be established that the law of distribution of the lifetime of the function is normal and, therefore, it is rational to apply the Laplace probability function.

The probability is calculated by the following formula:

$$P_{t \le T} = 0.5 + \Phi_0\left(\frac{T - M_t}{t}\right),$$

where $\Phi_0(z)$ – Laplace function;

P(t) –probability of realization of function for data center in the time interval T;

M_t, D_t –mathematical time of delay and dispersion.

Adapting the algorithm of the data center by serial configuration

One way to assess the quality of the data center is to define the function R (t) and the average time intervals between the errors - t_{cp}. Calculations are performed for a given specific timeframe, within which an active experiment is implemented (experiment consists in attempts to generate such errors). Time of stabilization of the analyzed system due to its setting and configuration, which consists of the approximation of the number of errors recorded for a given constant, can be used as Quality Score. The advantage of this method is the ability to assess the efficiency of the data center.

The value - t_{cp}, can be implemented by monitoring the data center state in a certain time interval and the intervals between errors. Furthermore the time between two consecutive errors tends to increase as more elements of the data centers are detected and corrected properly.

Error model may be based on the initial work that links R(t) and t_{cp}. The number of potential errors is statistically modelled in terms of the number of successful operations, the number of data center elements and seed errors. The additional assumption the rate of error being proportional to the number of the remaining not-configured data center elements can be added.

Assessment data center reliability is a function of R (t) and time, which is in between the errors of t_{cp}. These indicators make it possible to assess the resources that are spent on the system configuration, such as the time (labor costs debugging).

In this case the probabilities of standard functions are:

$$R(t) = P(t' > t);$$

$$F(t) = 1 - R(t);$$

$$f(t) = \frac{dF}{dt} = \frac{-dR(t)}{dt},$$

where t' is a random variable of error;

t – value of random variable;

$P(t < t')$ - Probability, used to determine that time of error lies outside the investigated interval

F(t) – distribution function (cumulative) that creates the values of error probability in the time interval from 0 to t.

R(t) – reliability function that creates the probability of error absence in the time interval from 0 to t.

It is also possible to use the risk function Z(t).This function is described in terms of probability of an event of error occurring in the interval t **to t +** Δ**t**.

The value is the probability of error being generated in the interval t to t + Δt.

With given constraint where error didn't occur until t:

$$p(t < t' < t + \frac{\Delta t}{t'}) = Z(t)\Delta t .$$

Solving the differential equation with initial conditions *R(0)*=1:

$$R(t) = e^{-\int_0^t Z(x)dx}$$

The mean time of error occurring can also be given by the following relation:

$$t_s = \int_0^\infty R(t)dt.$$

In the active experiment the cycles $T_1, T_2, ..., T_r$ represent the hours of correct functioning of the data center. With n total cycles, each (n-r) error is $t_1, t_2, ..., t_{n-r}$ hours of correct functioning before error occurring. Therefore the total number of hours is determined by:

$$H = \sum_{i=1}^{r} T_i + \sum_{i=1}^{n-r} t_i.$$

Investigating the number of errors equally we can determine to the given 1 hour of work:

$$\lambda = \frac{n - r}{H}.$$

The value of mean time within the interval between the 2 errors is calculated using:

$$t_s = \frac{1}{\lambda} = \frac{H}{n - r}.$$

Given the relationship between λ and t_s, we can carry out a quantitative evaluation of the degree of correct functioning of the data center.

With the assumptions that the amount of errors at the start of the experiment is constant and is decreasing while configuring the elements of the data center we can use the following model:

$$\varepsilon_r(\tau) = \frac{E\tau}{l_\tau} - \varepsilon_c(\tau),$$

where τ - time of experiment;

l_τ - number of elements of the data center;

E_τ - number of errors at $\tau = 0$;

$\varepsilon_c(\tau)$ - number of errors corrected by the time τ, normalized against l_τ;

$\varepsilon_r(\tau)$ - number of errors remaining at time normalized relative l_τ.

With the assumption that the total number pf possible errors are proportional to the number of errors occurred:

$$Z(t) = C\varepsilon_r(\tau),$$

where $Z(t)$ - function of the number of errors;

C - constant.

Considering all this we can conclude that the mean time between the errors can be calculated using:

$$R(t,\tau) = \exp[-C(\frac{E_\tau}{l_\tau} - \varepsilon_c(\tau))t],$$

$$t_s(\tau) = \frac{1}{C\left[\frac{E_\tau}{l_\tau} - \varepsilon_c(\tau)\right]}.$$

Considering the fact that assumption involves a known number of elements within the data center and a known statistics of errors the unknown elements are constants E_τ and C. These constants are determined in the process of experiment, in attempts to generate errors in 2 points of the time interval $\tau_1 < \tau_2$, chosen in such a way that $\varepsilon_c(\tau_1) < \varepsilon_c(\tau_2)$. Next step involves evaluation in times τ_1 and τ_2:

$$\frac{H_1}{(n_1 - r_1)} = \frac{1}{C\left[\frac{E_\tau}{l_\tau} - \varepsilon_c(\tau_1)\right]};$$

$$\frac{H_2}{(n_2 - r_2)} = \frac{1}{C\left[\frac{E_\tau}{l_\tau} - \varepsilon_c(\tau_2)\right]}$$

Resulting in:

$$E_\tau = \frac{l_\tau\left[\frac{\lambda_2}{\lambda_1}\varepsilon_c(\tau l) - \varepsilon_c(\tau_2)\right]}{\frac{\lambda_2}{\lambda_1} - 1};$$

$$C = \frac{\lambda_1}{\left[\left(\frac{E_\tau}{l_\tau} - \varepsilon_c(\tau_1)\right)\right]}.$$

The proposed adaptation methods solve the problem of organizing data center, protecting the virtual currency infrastructure so that the computer resources and power are integrated and are available as a unified service, which can be modified to fit the real requirements.

References

Akopova, S.E., Przhedetskaya, V.N., 2016. Imperative of State in the Process of Establishment of Innovational Economy in the Globalizing World. European Research Studies Journal, 19(2), 79-85.

Boldeanu , T.F and Tache, I. 2015. The Financial System of the EU and the Capital Markets Union. International Journal of Economics and Business Administration, 3(3), 41-51.

Dmitrishina, E.V. and Uskov, A.D. 2015. The Issues of Covering Science and Technical Policy of Modern Russia in the Strategic Planning Documents. European Research Studies Journal, 18 (4), 57 -74.

Epifanova, T., Romanenko, N., Mosienko, T., Skvortsova, T. and Kupchinskiy, A. 2015. Modernization of Institutional Environment of Entrepreneurship in Russia for Development of Innovation Initiative in Small Business Structures. European Research Studies Journal, 18(3), 137-148.

Fetai, B. 2015. Financial Integration and Financial Development: Does Financial Integration Matter? European Research Studies Journal, 18(2), 97-106.

Fomina J.S., Gutorov, H.A. 2014. Bitcoin: the threat of economic security or "e-gold" // Achieving high school science, number 8, pp. 262-267.

Information Letter CBR from, 2014. "On the use of" virtual currency" in transactions, in particular, Bitcoin" // Information and legal services "Consultant Plus".

Lomovtsev, D.A. 2014. Comparative characteristics of legal regulation of Bitcoin in different countries // Law and modern state, number 4, pp 5-9.

Molchanov, M.V. 2014. Cryptocurrency: concept and problems // Science time, № 10, pp 300-303.

Newsletter Rosfinmonitoring "On the use of cryptocurrency" // Information and legal services "Consultant Plus".

Oleander, N.V. 2015. Forensic characterization of electronic payment means and systems // Lex Russica, № 10, pp. 128-138.

Rusanov, Yu., Rovensky, A.Yu., Belyanchikova, T., Natocheeva, N.N. and Sysoeva, A.A. 2015. Social Priorities of Internal Banking Assortment (Products) Policy. European Research Studies Journal, 18(4), 307-320.

Rupeika-Apoga, R. and Nedovis Uraev, R. 2015. The Foreign Exchange Exposure of Non-Financial Companies in Eurozone: Myth or Reality? International Journal of Economics and Business Administration, 3(1), 54-66.

Thalassinos, I.E., Venediktova, B., Staneva-Petkova, D. 2013. Way of Banking Development Abroad: Branches or Subsidiaries. International Journal of Economics and Business Administration, 1(3), 69-78.

Thalassinos, I.E. and Stamatopoulos, V.T. 2015. The Trilemma and the Eurozone: A Pre-announced Tragedy of the Hellenic Debt Crisis. Journal of Economics and Business Administration, 3(3), 27-40.

Thalassinos, I.E. 2007. Trade Regionalization, Exchange Rate Policies and EU-US Economic Cooperation. European Research Studies Journal, 10(1-2), 111-118.

Tishchenko, E.N., Strokacheva, O.A. 2006. Evaluation of reliability parameters of a secure payment system e-commerce // Bulletin of the Rostov State University of Economics (RSUE), number 22, pp 115-122.

Tishchenko, E.N., Sharypova, T.N. 2014. Some approaches to protected data center virtual enterprise for integrated logistics support life cycle of complex products // Economics, number 114, pp 111-114.

Vovchenko, G.V., Ivanova, O., Kostoglodova, E. and Romanova, T. 2015. Institutional

Aspects of Provision of Sustainability of Budget System of the Russian Federation // Asian Social Science, vol.11, № 20.

Vovchenko, G.N., T. Panasenkova, T., I. Efremenko, I. 2015. Paradigm of the common economics space formation in the context of globalization // Mediterranean Journal of Social Sciences, Vol. No. 8 3 S.6.

Vovchenko, G.N., T. Panasenkova, T. 2013. Trends of Formation the Russia's Innovation Potential // World Applied Sciences Journal 27 (10): 1362-1366.

www.bitcoininfo.ru

www.fatf-gafi.org

www.fedsfm.ru